UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA
EASTERN DIVISION

In re DMS Health Technologies, Inc., Data Breach Litigation	Case No. 3:23-cv-204 CONSOLIDATED CLASS ACTION COMPLAINT JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiff**s** Stacy Kolkind and Constance Boyd (collectively, "Plaintiff**s**")**,** bring this class action against Defendant DMS Health Technologies, Inc. ("Defendant") on behalf of themselves and all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This is a class action for damages with respect to DMS Health Technologies, for its failure to exercise reasonable care in securing and safeguarding its patients' sensitive personal data—including name, date of birth, (personally identifying information" or "PII"), and date of service, physician name, and exam type, which is protected health information ("PHI", and collectively with Private Information, "Private Information" as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPPA").

2. Defendant is a business provider providing imaging services to various healthcare companies.

3. Defendant acquired, collected, and stored Plaintiffs and Class Members' PHI.

4. At all relevant times, Defendant knew or should have known, that Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI.

5. According to DMS's notice, on April 23, 2023, DMS became aware of suspicious activity related to certain computer systems and determined that there was unauthorized access to DMS's network between March 27 and April 24, 2023, and the unauthorized actor had the ability to access certain information stored on the network during the period of access.

6. On no later than April 24, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiffs and Class Members' PHI as hosted with Defendant, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiffs and Class Members' PHI.

7. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is unknown at this time but is in at least the tens of thousands, if not hundreds of thousands, based on the number of clientele Defendant serves.

8. Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"), which may include test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

9. The vulnerable and potentially exposed data at issue of Plaintiffs and the Class stored on Defendant's information network, includes, without limitation: names, dates of birth,

exam type, facility name, physician name, and treatment location/site location.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class Members' PHI was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

11. As a result, the PHI of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future.

12. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

14. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

15. Defendant is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally

availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiffs claims occurred within this District, and Defendant does business in this Judicial District.

THE PARTIES

Plaintiff Stacy Kolkind

17. Plaintiff Stacy Kolkind ("Plaintiff Kolkind") is an adult individual and, at all relevant times herein, a resident and citizen of Texas, residing in Mission, Texas. Plaintiff Kolkind is a victim of the Data Breach.

18. Plaintiff Kolkind was a patient of Mayo Clinic in Wisconsin, a client of DMS Health Technologies that shared Plaintiff Kolkind's Private Information.

19. Plaintiff Kolkind received services as late as Spring of this year.

20. Plaintiff Kolkind provided her Private Information to Mayo Clinic, a healthcare provider that relied on Defendant. Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information. If Plaintiff Kolkind had known that Defendant would not adequately protect her Private Information, she would not have entrusted Defendant with her Private Information or allowed Defendant to maintain this sensitive Private Information.

21. On or around April 22, 2023, a hacker gained access to Plaintiff Kolkind's email account. . Immediately thereafter, she noticed several unauthorized transactions on her Tremendous prepaid card, totaling at least $190. Additionally, on or around April 23, 2023,

Plaintiff Kolkind's Southwest Airlines voucher[1] (valued at $200), was redeemed for the full amount without her knowledge and permission.

22. Plaintiff Kolkind received a notice letter from DMS on September 30, 2023, stating that her personal information had been exposed.

Plaintiff Constance Boyd

23. Plaintiff Constance Boyd ("Plaintiff Boyd") is an adult individual and, at all relevant times herein, a resident and citizen of Minnesota, residing in Hinckley, Minnesota. Plaintiff is a victim of the Data Breach.

Defendant DMS Health Technologies, Inc.

24. Defendant DMS Health Technologies, Inc., is a North Dakota corporation with its principal place of business located at 728 East Beaton Dr., Suite 101, West Fargo, ND 58078.

CLASS ACTION ALLEGATIONS

25. Plaintiffs brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the Class:

> All individuals within the United States of America whose PHI was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on or around April 23, 2023.

26. Additionally, Plaintiff Kolkind brings this action in the alternative on behalf of themselves and the following Class Subclass"):

> All individuals within Wisconsin whose PHI was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on or around April 23, 2023.

27. Additionally, Plaintiff Boyd brings this action in the alternative on behalf of

[1] During the relevant period, Plaintiff Kolkind had two (2) Southwest Airlines vouchers.

themselves and the following Class ("Minnesota Subclass"):

> All individuals within Minnesota whose PHI was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on or around April 23, 2023.

28. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

29. Plaintiffs reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

30. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

31. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible.

32. Commonality: Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiffs and the Classes to

exercise due care in collecting, storing, using, and/or safeguarding their PHI;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PHI had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI of Plaintiffs and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI of Plaintiff and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or

declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

33. Typicality: Plaintiffs claims are typical of the claims of the Class. Plaintiffs and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

34. Adequacy of Representation: Plaintiffs in this class action is an adequate representative of each of the Class in that the Plaintiffs have the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

35. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiffs anticipate no management difficulties in this litigation.

36. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

37. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests

adequately.

38. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

39. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiffs.

40. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PHI of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

41. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Defendant's Failed Response to the Breach

42. Not until after months it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI Defendant confirmed was potentially compromised as a result of the Data Breach.

43. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the Data Breach on or

around April 23, 2023, and completed a review thereafter.

44. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs and Class Members' PHI with the intent of engaging in the misuse of the PHI, including marketing, and selling Plaintiffs and Class Members' PHI.

45. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiffs and Class Members' PHI confidential and to protect such PHI from unauthorized access.

46. Plaintiffs and Class Members were required to provide their PHI to Defendant in order to receive healthcare, and as part of providing healthcare, Defendant created, collected, and stored Plaintiffs and Class Members with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. Despite this, Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PHI going forward.

48. Plaintiffs and Class Members are, thus, left to speculate as to where their PHI ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

49. Unauthorized individuals can now easily access the PHI of Plaintiffs and Class Members.

Defendant Collected/Stored Class Members' PHI

50. Defendant acquired, collected, and stored and assured reasonable security over Plaintiffs and Class Members' PHI.

51. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PHI.

52. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

53. By obtaining, collecting, and storing Plaintiffs and Class Members' PHI, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiffs and Class Members' PHI from unauthorized disclosure.

54. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PHI.

55. Plaintiffs and Class Members relied on Defendant to keep their PHI confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

56. Defendant could have prevented the Data Breach, which potentially began as early as March 27, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs and Class Members' PHI.

57. Defendant's negligence in safeguarding Plaintiffs and Class Members' PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

58. Yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs and Class Members' PHI from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

59. Defendant's failure to adequately secure Plaintiffs and Class Members' sensitive data breaches duties it owes Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiffs' and Class Members' data. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

60. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

61. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

62. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

63. HIPAA requires Defendant to "comply with the applicable standards,

implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

64. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

65. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

66. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

67. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of the breach."

68. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[2]

69. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

70. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PHI of Plaintiff and Class Members.

71. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PHI was adequately secured and protected.

72. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PHI in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

73. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

74. Defendant owed a duty to Plaintiffs and Class Members to act upon data security

[2] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

warnings and alerts in a timely fashion.

75. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI from theft because such an inadequacy would be a material fact in the decision to entrust this PHI to Defendant.

76. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

77. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PHI and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

78. PHI are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

79. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[3]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[4]; and other sources report that criminals can also

[3] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed October 27, 2023).

[4] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed October 27, 2023).

purchase access to entire company data breaches from $999 to $4,995.[5]

80. Identity thieves can use PHI, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

81. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

82. Here, Defendant knew of the importance of safeguarding PHI and of the foreseeable consequences that would occur if Plaintiffs and Class Members' PHI were stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach of this magnitude.

83. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law

[5] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed October 27, 2023).
[6] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed October 27, 2023).

duties to Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

84. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

PLAINTIFFS' INDIVIDUAL EXPERIENCES

Plaintiff Stacy Kolkind's Experience

85. Plaintiff Kolkind was a patient at Mayo Clinic in Eau Claire, Wisconsin where she received mobile imaging provided by DMS.

86. Plaintiff Kolkind provided her Private Information to Mayo Clinic between March 2012 through June 2021. DMS received Plaintiff Kolkind's Private Information during this period .

87. Between March 27, 2023, and April 24, 2023, DMS's network that housed Plaintiff Kolkind's Private Information was compromised.

88. Like all Class Members, Plaintiff Kolkind has faced and will continue to face an impending and substantial risk of future harm due to Defendant's completely lax and ineffectual data security measures, as further set forth herein. Some of these harms will include fraudulent charges, charges, loans or medical procedures ordered in her name without her permission, and

targeted advertising without her consent.

89. Some of these consequences may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue through the misuse of Plaintiff Kolkind's Private Information.

90. In fact, Plaintiff Kolkind has already suffered hardship because of the Data Breach. On or around April 22, 2023, a hacker gained access to Plaintiff Kolkind's email account. Immediately thereafter, she noticed several unauthorized transactions on her Tremendous prepaid card, totaling at least $190.

91. On or around April 23, 2023, Plaintiff Kolkind's Southwest Airlines voucher (valued at $200) was redeemed for the full amount without her knowledge or permission.

92. Both hackings of Plaintiff Kolkind's Private Information occurred within the window of the DMS data breach.

93. DMS informed Plaintiff Kolkind that it had exposed her Private Information in a notice letter dated September 25, 2023.

94. Plaintiff Kolkind received the DMS notice letter on September 30, 2023.

95. To obtain medical services, Plaintiff was required to provide her Private Information to Defendant.

96. At the time of the Data Breach, DMS retained Plaintiff Kolkind's Private Information in its system.

97. Plaintiff Kolkind is very careful about sharing her sensitive Private Information

98. Plaintiff Kolkind immediately took steps to protect and vindicate her rights, including initiating this litigation. Due to the recency of her discovery, Plaintiff Kolkind will be expending appreciable time and energy monitoring her accounts and remaining alert of fraud

and/or identity theft attempts.

99. As a result of the Data Breach, and at the direction of Defendant's notice letter, Plaintiff Kolkind made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: notifying Tremendous and Southwest Airlines, researching and verifying the legitimacy of the Data Breach, as well as reaching out to counsel, and checking her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Kolkind has spent significant time remedying the Breach–valuable time Plaintiff otherwise would have spent on other activities, including (but not limited to) work and/or recreation.

100. Plaintiff Kolkind suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of her Private Information; and (vi) the continued and increased risk of fraud and identity theft.

101. The Data Breach has caused Plaintiff Kolkind to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

102. Thus, Plaintiff Kolkind anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Breach As a result of the Data Breach, Plaintiff Kolkind is presently at risk and will continue to be at i*ncreased* risk of identity theft and fraud for years to come.

103. Due to the increased risks of identity theft and/or fraud, Plaintiff Kolkind's family has purchased and will continue to purchase credit monitoring services at a cost of $24.99/month.

104. Plaintiff Kolkind has a continuing interest in ensuring that her Private Information,

which (upon information and belief), remains in Defendant's possession, is safeguarded from future breaches.

Plaintiff Boyd's Experience

105. Plaintiff Boyd was a client of Essentia Health Sandstone's, a client of Defendant's, and her information was stored with Defendant as a result of their dealings with Defendant and Essentia Health Sandstone.

106. As required to obtain services from Defendant, Plaintiff Boyd provided Defendant with highly sensitive personal and health information, who then possessed and controlled it.

107. As a result, Plaintiff Boyd's information was among the data accessed by an unauthorized third-party in the Data Breach.

108. At all times herein relevant, Plaintiff Boyd is and was a member of each of the Classes.

109. Plaintiff Boyd received a letter from Defendant, dated October 17, 2023, stating that her PHI was involved in the Data Breach (the "Notice").

110. Plaintiff Boyd was unaware of the Data Breach—or even that Defendant had possession of her data until receiving that letter.

111. As a result, Plaintiff Boyd was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self- monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach.

112. Plaintiff Boyd was also injured by the material risk to future harm she suffers based on Defendant's breach; this risk is imminent and substantial because Plaintiff Boyd's data has been exposed in the breach, the data involved, including healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

113. Plaintiff Boyd suffered actual injury in the form of damages to and diminution in the value of her PHI—a condition of intangible property that she entrusted to Defendant, which was compromised in and as a result of the Data Breach.

114. Plaintiff Boyd, as a result of the Data Breach, has increased anxiety for her loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PHI.

115. Plaintiff Boyd has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PHI, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

116. Plaintiff Boyd has a continuing interest in ensuring that her PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of Plaintiffs and the Class)

117. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

118. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI and to use

commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PHI of Plaintiffs and Class Members in its computer systems and on its networks.

119. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI in its possession;

b. to protect Plaintiffs and Class Members' PHI using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI.

120. Defendant knew that the PHI was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

121. Defendant knew, or should have known, of the risks inherent in collecting and storing PHI, the vulnerabilities of its data security systems, and the importance of adequate security.

122. Defendant knew about numerous, well-publicized data breaches.

123. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs and Class Members' PHI.

124. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI that Plaintiffs and Class Members had entrusted to it.

125. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI.

126. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PHI contained therein.

127. Plaintiffs and Class Members' willingness to entrust Defendant with their PHI was predicated on the understanding that Defendant would take adequate security precautions.

128. Moreover, only Defendant had the ability to protect its systems and the PHI is stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

129. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

130. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs and Class Members' PHI and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiffs, and/or the remaining Class Members.

131. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI of Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Plaintiffs and Class Members' PHI had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI;

d. by failing to provide adequate supervision and oversight of the PHI with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI of Plaintiffs and Class Members, misuse the PHI and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PHI longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class Members' PHI;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiffs and Class Members' PHI and monitor user

behavior and activity in order to identify possible threats.

132. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

133. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages.

134. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI to Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI.

135. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and Class Members and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach.

136. To date, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class Members.

137. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PHI, and to access their medical records and histories.

138. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI of Plaintiffs and Class Members and the harm suffered,

or risk of imminent harm suffered by Plaintiffs and Class Members.

139. Plaintiffs and Class Members' PHI was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

140. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

141. The damages Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

142. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PHI in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and

Class Members.

143. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

144. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

145. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

146. Through its course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' PHI.

147. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when they first entered into the services agreement with Defendant.

148. Defendant required Plaintiffs and Class Members to provide and entrust their PHI as a condition of obtaining Defendant's services.

149. Defendant solicited and invited Plaintiffs and Class Members to provide their PHI as part of Defendant's regular business practices.

150. Plaintiffs and Class Members accepted Defendant's offers and provided their PHI to Defendant.

151. As a condition of being clients of Defendant, Plaintiffs, and Class Members provided and entrusted their PHI to Defendant.

152. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

153. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

154. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide imaging services to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PHI provided to obtain such benefits of such services. In exchange, Plaintiffs and Class Members agreed to pay money for these services, and to turn over their Private Information.

155. Both the provision of imaging services and the protection of Plaintiffs' and Class Members' PHI were material aspects of these implied contracts.

156. The implied contracts for the provision of imaging services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' PHI—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice and Data Breach notification letter.

157. Defendant's express representations, including, but not limited to the express

representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and protect the privacy of Plaintiff's and Class Members PHI.

158. Consumers of imaging services value their privacy, the privacy of their dependents, and the ability to keep their PHI associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their PHI to Defendant and entered into these implied contracts with Defendant without an understanding that their PHI would be safeguarded and protected. Nor would they have entrusted their PHI to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

159. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PHI to Defendant, in exchange for, amongst other things, the protection of their PHI.

160. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

161. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their PHI and by failing to provide timely and accurate notice to them that their PHI was compromised as a result of the Data Breach.

162. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

163. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described

in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

164. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

165. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

166. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Class)

167. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

168. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

169. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

170. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PHI and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

171. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

172. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

173. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

174. Defendant, prior to and at the time Plaintiffs and Class Members entrusted their PHI to Defendant for the purpose of obtaining health services, caused Plaintiffs and Class Members to reasonably believe that Defendant would keep such PHI secure.

175. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

176. Defendant was also aware that, if the substandard condition of and vulnerabilities

in its information systems were disclosed, it would negatively affect Plaintiffs and Class Members' decisions to seek services therefrom.

177. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

178. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiffs and Class Members the ability to make a rational and informed purchasing and health care decision and took undue advantage of Plaintiffs and Class Members.

179. Defendant was unjustly enriched at the expense of Plaintiffs and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

180. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

181. Plaintiffs and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs and Class Members may seek restitution.

COUNT FIVE
Breach of Contract:
Third Party Beneficiary
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs re-allege and incorporate by reference herein all of the allegations fully set forth herein.

183. Plaintiffs and Class Members provided and entrusted Defendant with certain PHI, including, without limitation, name, date of birth, date of service, physician name, and exam type.

184. Plaintiffs and the Class entrusted their PHI to Defendant or Defendant's clients on the premise and with the understanding that Defendant would safeguard their information, use their PHI for business purposes only, and/or not disclose their PHI to unauthorized third parties.

185. As a condition of receiving services from Defendant's clients, Plaintiffs, and the Class entrusted their personal and medical information to Defendant's clients, which gave rise to a duty to safeguard that information.

186. Defendant's clients are laboratories, physicians' offices, hospitals, and other healthcare providers.

187. Defendant and Defendant's clients contracted for imaging services, among other things.

188. Upon information and belief, these contracts included, in part, promises to provide data retention and security services, which include compliance with data protection statutes and industry-wide standards for the protection of PHI.

189. Thus, Defendant promised to discharge Defendant's clients' duties to safeguard the personal and medical information of Plaintiffs and the Class.

190. Upon Plaintiffs information and belief, Defendant's contracts with clients, among other things, promised to take reasonable measures to safeguard and protect such information for the benefit of Plaintiffs and the Class.

191. Similarly, when Defendant's clients provided the Plaintiffs and Class's PHI to Defendant, Plaintiffs and the Class were the intended third party beneficiaries of Defendant's promise to safeguard the data.

192. Defendant breached the contracts it entered by failing to provide reasonable data security measures.

193. Defendant solicited and invited Plaintiffs and Class Members or their respective healthcare providers to provide their PHI as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PHI to Defendant.

194. As a direct and proximate result of Defendant's above-described breach of contract with its customers, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

195. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT SIX
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

196. Plaintiffs realleges and incorporates by reference herein all paragraphs as though fully set forth herein.

197. Plaintiffs and the Class provided and entrusted Defendant with PHI.

198. Plaintiffs and the Class entrusted their PHI to Defendant or Defendant's clients on the premise and with the understanding that defendant would safeguard their information, use their PHI for business purposes only, and/or not disclose their PHI to unauthorized third parties.

199. Defendant owed a duty to the individuals for whom it maintained and stored information, including Plaintiffs and the Class, to keep their PHI contained as a part thereof, confidential.

200. Defendant failed to protect and actually or potentially released to unknown and unauthorized third parties the PHI of Plaintiffs and the Class.

201. Defendant allowed unauthorized and unknown third parties to actually or potentially access and examine the PHI of Plaintiffs and the Class, by way of Defendant's failure to protect the PHI.

202. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI of the Plaintiffs and the Class is highly offensive to a reasonable person.

203. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their PHI to Defendant as part of Plaintiffs and the Class's relationships with Defendant, but privately with an intention that the PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and not be disclosed without their authorization.

204. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable

person.

205. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

206. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

207. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was accessed by to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

208. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

209. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

COUNT SEVEN
Violation of the Wisconsin Notice of Unauthorized Acquisition of Personal Information
Wis. Law. § 134.98, *et. seq.*
(On Behalf of Plaintiff Kolkind and the Wisconsin Subclass)

210. Plaintiff Kolkind repeats and realleges all paragraphs as though fully set forth herein.

211. Defendant is an entity under §134.98(1)(a) because Defendant "conducts business in this state and maintains personal information in the ordinary course of business."

212. Private Information as alleged herein in this complaint is covered as "Personal Information" in this statute §134.98(1)(b). Defendants exposed individuals first and last name in combination with an individual's unique biometric data as exposed via exam type

213. Under §134.98(3), an entity is required to provide notice "not to exceed 45 days after the entity learns of the acquisition of personal information." Defendant did not comply with this statute. Defendant provided notice to Plaintiff Kolkind almost five months after it first learned of the acquisition of personal information.

214. Plaintiff Kolkind and Class Members exercise their rights granted under § 134.98(4) that Defendant's actions "may be evidence of negligence or a breach of a legal duty.

COUNT EIGHT
Violation of North Dakota's Privacy of Consumer Financial and Health Information
N.D.C.C. § 45-14-01 *et. seq*
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs repeat and reallege all paragraphs as though fully set forth herein.

216. Under the scope of the statute, Plaintiffs and Class Members use of DMS services for personal healthcare qualify as "individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family, or household purposes from licensees… ." § 41-14-02(a). Plaintiffs and Class Members private health information is covered under this statute as "nonpublic personal health information." § 41-14-02(b), (21). "Health information" relates to the "provision of health care to an individual." § 41-14-02(15).

217. Health care" includes "diagnostic care", "services", or "counseling" that "relates to the physical, mental, or behavioral condition of an individual; or affects the structure or

function of the human body or any part of the human body…." DMS imaging services suffice are providing healthcare under this statute. § 41-14-02(13).

218. "Health care provider" is a health care practitioner or healthcare facility under this statute as Defendant is one of the nation's largest providers of mobile imaging products. § 41-14- 02(14).

219. Defendant violated § 45-01-14-17 when it disclosed Plaintiffs and Class Member's nonpublic personal health information without their authorization. The statute clearly says Defendant "shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

COUNT NINE
Declaratory Relief
(On Behalf of Plaintiffs and the Class)

220. Plaintiffs repeat and reallege all paragraphs as though fully set forth herein.

221. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

222. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs and the Class remain

at imminent risk that further compromises of their Private Information will occur in the future.

223. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' Private Information.

224. Defendant still possesses the Private Information of Plaintiffs and the Class.

225. Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

226. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

227. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial.

228. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs to Defendant, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

229. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach to Defendant, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other consumers whose Personal Information would be further

compromised.

230. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant owed and continues to owe a duty to implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks;
- and routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT TEN
Violation of the Minnesota Health Records Act
Minn. Stat. §§ 144.291 and 144.293
(On Behalf of Plaintiff Boyd and the Minnesota Subclass)

231. Plaintiff Boyd incorporates by reference all previous allegations as though fully set forth herein.

232. Under the Minnesota Health Records Act, "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment for the provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c) (the "MHRA").

233. The PHI of Plaintiff Boyd and the Class that was released in the Data Breach involved health records as that term is defined in the MHRA.

234. Plaintiff Boyd and the Class are "patients" as that term is defined under the MHRA at all times relevant to this action under Minn. Stat. § 144.291, subd. 2(g).

235. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

236. Via the Data Breach, DMS released Plaintiff Boyd's and the Class's health records.

237. Neither Plaintiff Boyd nor the Class consented to have their health records released in the Data Breach.

238. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees. Minn. Stat. § 144.298, subd. 2. As a result of DMS's violations of the MHRA, Plaintiff Boyd and the other Class members seek all damages authorized by law, including compensatory damages plus costs, and reasonable attorney fees.

COUNT ELEVEN
Violation of N.D. Cent. Code § 51-22-02
(On Behalf Plaintiffs and the Class)

239. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

240. North Dakota Century Code § 51-22-02 provides: "No business entity which charges a fee for data processing services performed may disclose in whole or in part the contents of any record . . . which is prepared or maintained by such business entity to any person, other than the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity."

241. Defendant is a business entity under § 51-22-02 because it is a company with its principal place of business in North Dakota. Defendant also charges a fee for, *inter alia*, performing "systematic sequence[s] of operations, including but not limited to bookkeeping functions, inventory control, storage, or manipulation and retrieval of management or personnel information." N.D. Cent. Code § 51-22-01. These actions are performed "upon data by electronic devices which perform logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses." *Id.*

242. Defendant disclosed Plaintiffs and Class Members' PI to third parties without their consent by failing to take appropriate measures to safeguard and protect that PI amidst a foreseeable risk of a cybersecurity attack, resulting in the Data Breach.

243. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Class Members as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation:

a. actual identity theft;

b. the compromise, publication, and/or theft of their PI;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

e. costs associated with placing freezes on credit reports;

f. the continued risk to their PI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI of its current and former employees and customers in its continued possession; and

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

244. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages due to the violations of N.D.C.C. § 51-22-02 and Defendant is thus liable in an amount equal to the actual damages sustained, but in no case less than five hundred dollars to each Plaintiff and Class Member, including but not limited to the damages set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the Class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages,

as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

5. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PHI of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PHI;

e. requiring Defendant to engage independent third-party security auditors

and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiffs' and Class Members' PHI on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI, as well as protecting the PHI of Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting private health information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess

whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiffs, individually and on behalf of the Class and/or Subclasses, hereby demands a trial by jury for all issues triable by jury.

Dated: March __, 2024

Respectfully submitted,

By: */s/ [counsel]*

SOLBERG STEWART MILLER
Todd Miller
N.D. bar # 06625
PO Box 1897
1123 5th Ave. South
Fargo, North Dakota 58107
T: 701.237.3166
miller@solberglaw.com

Interim Liaison Counsel

MIGLIACCIO & RATHOD LLP
Nicholas A. Migliaccio (*pro hac vice*)
Jason S. Rathod (*pro hac vice*)
412 H Street N.E., Suite 302
Washington, D.C. 20002

T: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com

LAUKAITIS LAW LLC
Kevin Laukaitis
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Interim Co-lead Counsel

SCIOLLA LAW FIRM LLC
Andrew J. Sciolla*
Land Title Building
100 S. Broad Street, Suite 1910
Philadelphia, PA 19110
T: 267-328-5245
F: 215-972-1545
andrew@sciollalawfirm.com

**Pro Hac Vice admission forthcoming*

Additional Plaintiff's Counsel